

**IN THE UNITED STATES DISTRICT COURT  
FOR THE NORTHERN DISTRICT OF MISSISSIPPI  
GREENVILLE DIVISION**

**DEIDRA BYAS and  
K'ACIA DRUMMER, individually  
and on behalf of all others  
similarly situated,**

**Plaintiffs,**

**v.**

**Case No. 4:17cv130-DMB-JMV**

**EQUIFAX, INC.,**

**Defendant.**

**PLAINTIFFS' CLASS ACTION COMPLAINT**

**JURY TRIAL DEMANDED**

**THE PARTIES**

1. Deidra Byas is an individual consumer residing in the Cleveland, Mississippi area and K'acia Drummer is an individual consumer residing in the Cleveland, Mississippi area. Plaintiffs are victims of the date breach and have spent time and effort monitoring their financial accounts.

2. Equifax Inc. (Equifax) is a multi-billion dollar Delaware corporation with its principal place of business located at 1550 Peachtree Street NE Atlanta, Georgia 30309. Equifax, Inc. may be served through its registered agent, Shawn Baldwin, at its principal office address identified above, that provides credit information services to

millions of businesses, governmental units, and consumers across the globe. Equifax operates through various subsidiaries including Equifax Information Services, LLC, and Equifax Consumer Services, LLC aka Equifax Personal Solutions aka PSOL. Each of these entities acted as agents of Equifax or in the alternative, acted in concert with Equifax as alleged in this complaint.

#### **JURISDICTION AND VENUE**

3. This Court has jurisdiction under the Class Action Fairness Act 28 U.S.C. § 1332 because the parties are citizens of different states and the amount in controversy exceeds \$5 million exclusive of interest and costs.

4. Venue is proper under 28 U.S.C. § 1391 because a substantial number of Mississippi consumers with credit and personal information stored by Equifax live in the Northern district area. There are more than 100 putative class members. And, at least some members of the proposed Class have a different citizenship from Equifax.

#### **CLASS ALLEGATIONS**

5. Plaintiffs file this complaint as a national class action lawsuit.

6. Pursuant to Fed. R. Civ. P. 23(a), (b)(2), (b)(3) and (c)(4), Plaintiffs seeks certification of a Nationwide class defined as, “all persons residing in the United States whose personally identifiable information was acquired by unauthorized persons in the data breach announced by Equifax in September 2017 also known as the “Nationwide Class”.

7. Pursuant to Fed. R. Civ. P. 23, and in the alternative to claims asserted on behalf of the Nationwide Class, Plaintiffs assert claims under the laws of the individual States, and on behalf of separate statewide classes, defined as, all persons residing in Mississippi whose personally identifiable information was acquired by unauthorized

persons in the data breach announced by Equifax in September 2017 also known as the "Statewide Classes".

8. The Mississippi class consists of Mississippi consumers who:

a) Had personal or credit data collected and stored by Equifax in the past year, and

b) Who were subject to risk of data loss and credit harm and identity theft or had to pay for third-party credit monitoring services as a result of Equifax's negligent data breach from May to July 2017.

9. Excluded from the class are all attorneys for the class, officers and members of Equifax, including officers and members of any entity with an ownership interest in Equifax, any judge who sits on the case, and all jurors and alternate jurors who sit on the case.

10. Plaintiffs hereby reserve the right to amend or modify the class definition with greater specificity or division after having had an opportunity to conduct discovery.

11. The class is so numerous that joinder is impracticable. Upon information and belief, the Mississippi class alone includes hundreds of thousands and possibly a million or more of consumers based on Equifax's estimate that its data breach affected 143 million consumers nationwide.

12. A class action is superior to other methods for fair and efficient adjudication of this case because common questions of law and fact predominate over other factors affecting only individual members, as far as plaintiffs know, no class action that purports to include Mississippi consumers suffering the same injury has been commenced in Mississippi ,individual class members have little interest in controlling the litigation, due to the high cost of actions, the relatively small amounts of damages, and because plaintiffs

and their attorneys will vigorously pursue the claims. The forum is desirable because a substantial number of consumers in Mississippi who suffered injury caused by Equifax's negligence reside in the Northern District of Mississippi.

13. Common questions of fact and law predominate over any questions affecting only individual class members. Common questions include whether plaintiffs and the Mississippi class members are entitled to equitable relief, whether Equifax acted negligently, and whether plaintiffs and the Mississippi class members are entitled to recover money damages.

14. A class action will be an efficient method of adjudicating the claims of the class members who have suffered relatively small damages, as a result of the same conduct by Equifax. In the aggregate, class members have claims for relief that are significant in scope relative to the expense of litigation. The availability of defendant's consumer data will facilitate proof of class claims, processing class claims, adequate assessment of damages and distributions of any recoveries.

15. Finally, all members of the proposed Classes are readily ascertainable. Equifax has access to information regarding the Data Breach, the time-period of the Data Breach, and which individuals were potentially affected. Using this information, the members of the Class can be identified and their contact information ascertained for purposes of providing notice to the Class.

#### **NATURE OF THE CASE**

16. On September 7, 2017, Equifax announced for the first time that from May to July 2017, its database storing Plaintiffs' credit and personal identification information had been hacked by unauthorized third parties, subjecting them to increased risk of credit harm, misuse and identify theft.

17. Equifax is one of three nationwide credit-reporting companies that track and rates the financial history of U.S. consumers. The companies are supplied with data about loans, loan payments and credit cards, as well as information on everything from child support payments, credit limits, missed rent and utilities payments, addresses and employer history. All this information, and more factors into credit scores.

18. Plaintiffs' bring this complaint as a class action case against Defendant Equifax for its failures to secure and safeguard approximately 143 million consumers' credit and personal identification information which Equifax collected from various sources during the operation of its business as a consumer credit reporting agency, and for failing to provide timely, accurate, specific and adequate notice to Consumer Plaintiffs and other Class members that their credit and personal identification information had been stolen and compromised.

19. Equifax has acknowledged that a cybersecurity/data breach incident potentially impacting approximately 143 million U.S. consumers. It has also acknowledged that unauthorized persons exploited a U.S. website application vulnerability to gain access to certain files. Equifax claims that based on its investigation, the unauthorized access occurred from mid-May through July 2017. The information accessed primarily includes names, Social Security numbers, birth dates, addresses and, in some instances, driver's license numbers. In addition, credit card numbers for approximately 209,000 U.S. consumers, and certain dispute documents with personal identifying information for approximately 182,000 U.S. consumers, were accessed.

20. Equifax has acknowledged that it discovered the unauthorized access on July 29 2017, but has failed to inform the public why it delayed notification of the Data Breach to consumers. Instead, three (3) of the Equifax's executives sold approximately \$

\$2 million dollars in stock days after the hack was discovered and before the public disclosure of the breach

21. The credit and personal identification information for Plaintiffs and the class of consumers they seek to represent was compromised due to Equifax's acts and omissions and their failure to maintain adequate technological safeguards to properly protect against unauthorized access by hackers.

22. Like other companies and agencies that are in the consumer credit reporting business, Equifax could have prevented this Data Breach. Data breaches at other credit reporting agencies have occurred.

23. The Data Breach was the inevitable result of Equifax's inadequate approach to data security and the protection of the credit and personal identification information that it collected during the course of its business operations. The hackers gained access by exploiting a vulnerability on one of the company's U.S.-based servers, that are approximately 12-14 years old, which allowed them to retrieve "certain files."

24. Equifax totally disregarded the rights of Plaintiffs and Class members by intentionally, willfully, recklessly, or negligently failing to take adequate and reasonable measures to ensure its data systems were protected, failing to disclose to its customers the material fact that it did not have adequate computer systems and security practices to safeguard the credit and personal identification information, failing to take available steps to prevent and stop the breach from ever happening, and failing to monitor and detect the breach on a timely basis.

25. As a result of the Equifax Data Breach, the credit and personal identification of the Plaintiffs and Class members has been exposed to criminals for misuse. The injuries

suffered by Plaintiffs and Class members, or likely to be suffered by Plaintiffs and Class members as a direct result of the Equifax Data Breach include:

- a. unauthorized use of their credit and personal identification information;
- b. theft of their personal and financial information;
- c. costs associated with the detection and prevention of identity theft and unauthorized use of their financial accounts;
- d. damages arising from the inability to use their PII;
- e. loss of use of and access to their account funds and costs associated with inability to obtain money from their accounts or being limited in the amount of money they were permitted to obtain from their accounts, including missed payments on bills and loans, late charges and fees, and adverse effects on their credit including decreased credit scores and adverse credit notations;
- f. costs associated with time spent and the loss of productivity or the enjoyment of one's life from taking time to address and attempt to ameliorate, mitigate and deal with the actual and future consequences of the Data Breach, including finding fraudulent charges, purchasing credit monitoring and identity theft protection services, and the stress, nuisance and annoyance of dealing with all issues resulting from the Equifax Data Breach;
- g. the imminent and certainly impending injury flowing from potential fraud and identify theft posed by their PII being placed in the hands of criminals and already misused via the sale of Plaintiffs' and Class members' information on the Internet black market;
- h. damages to and diminution in value of their PII entrusted to Equifax for the sole purpose of purchasing products and services from Equifax; and
- i. the loss of Plaintiff's and Class members' privacy.

26. The injuries to the Plaintiffs and Class members were directly and proximately caused by the failure to implement or maintain adequate data security measures for protecting their credit and personal identification information stored by Equifax.

27. Further, Plaintiffs retain a significant interest in ensuring that their credit and personal information, which, while stolen, remains in the possession of Equifax is protected from further breaches, and seek to remedy the harms they have suffered on behalf of themselves and similarly situated consumers whose credit and personal information was stolen as a result of the Equifax Data Breach.

28. Plaintiffs bring this action to remedy these harms on behalf of themselves and all similarly situated individuals whose credit and personal information was compromised and potentially accessed by hackers during the Data Breach. Plaintiffs seek the following remedies, among others: statutory damages under the Fair Credit Reporting Act (“FCRA”) and state consumer protection statutes, reimbursement of out-of-pocket losses, other compensatory damages, further and more robust credit monitoring services with accompanying identity theft insurance, and injunctive relief including an order requiring Equifax to implement improved data security measures.

29. That certain consumers that may be affected by the hacking of Equifax’s servers may not be aware or informed because Equifax gets its data from credit card companies, banks, retailers, and lenders who report on the credit activity of individuals to credit reporting agencies, as well as by purchasing public records.

30. Plaintiffs suffered actual injury and harm in the form of damages to and a decline in the value of their credit score and unauthorized access and misuse of their personal identification information

31. Additionally, Plaintiffs has suffered imminent and impending injury arising from the substantially increased risk of future fraud, identity theft and misuse posed by their credit and personal identification information being placed in the hands of criminals who have already, or will imminently, misuse such information.

32. Moreover, Plaintiffs has a continuing interest in ensuring that their private information, which remains in the possession of Equifax, is protected and safeguarded from future breaches.

33. At all relevant times, Equifax was well-aware, or reasonably should have been aware, that the personal identification information collected, maintained and stored in the POS systems is highly sensitive, susceptible to attack, and could be used for wrongful purposes by third parties, such as identity theft and fraud.

34. At all relevant times, Equifax knew, or reasonably should have known, of the importance of safeguarding credit and personal identification information and of the foreseeable consequences that would occur in the event of a data breach, including, specifically, the significant harm that would be imposed on individuals as a result of a breach of its servers.

35. Equifax's approach to maintaining the privacy and security of the credit and personal information of Plaintiffs and Class members was at the very least, negligent. Equifax chose to ignore the wide array of the publicly available knowledge of repeated hacks, misuse and compromises of credit and personal identification of consumers that occurs in the unauthorized use and access of said information by third parties, Plaintiffs and Class members now face years of constant surveillance of their financial and personal records, monitoring, and loss of rights. The Class is incurring and will continue to incur

such damages in addition to any fraudulent use of their credit and personal identification information.

36. The personal identification information of Plaintiffs and Class members is private and sensitive in nature and was left inadequately protected by Equifax. Equifax did not obtain Plaintiffs' and Class members' consent to disclose their personal identification information to any other person as required by applicable law and industry standards.

37. The Equifax Data Breach was a direct and proximate result of Equifax's failure to properly safeguard and protect Plaintiffs' and Class members' PII from unauthorized access, use, and disclosure, as required by various state and federal regulations, industry practices, and the common law, including Equifax's failure to establish and implement appropriate administrative, technical, and physical safeguards to ensure the security and confidentiality of Plaintiffs' and Class members' PII to protect against reasonably foreseeable threats to the security or integrity of such information.

38. Equifax had the resources to prevent a breach, but neglected to adequately invest in data security, despite the growing number of well-publicized data breaches.

39. As a direct and proximate result of Equifax's wrongful actions and inaction and the resulting Data Breach, Plaintiffs and Class members have been placed at an imminent, immediate, and continuing increased risk of harm from identity theft and identity fraud, requiring them to take the time which they otherwise would have dedicated to other life demands such as work and effort to mitigate the actual and potential impact of the Data Breach on their lives including, inter alia, by placing "freezes" and "alerts" with credit reporting agencies, contacting their financial institutions, closing or modifying financial accounts, closely reviewing and monitoring their credit reports and accounts for

unauthorized activity, and filing police reports. This time has been lost forever and cannot be recaptured

**COUNT I NEGLIGENCE**

**(ON BEHALF OF PLAINTIFFS AND THE NATIONWIDE CLASS, OR,  
ALTERNATIVELY, PLAINTIFFS AND THE SEPARATE STATEWIDE  
CLASSES)**

40. Plaintiffs restate and reallege Paragraphs 1 through 37 as if fully set forth herein.

41. Upon accepting and storing the personal identification information of Plaintiffs and Class Members in its computer systems and on its networks, Equifax undertook and owed a duty to Plaintiffs and Class Members to exercise reasonable care to secure and safeguard that information and to use commercially reasonable methods to do so. Equifax knew that the PII was private and confidential and should be protected as private and confidential.

42. Equifax owed a duty of care not to subject Plaintiffs, along with their credit and personal identification information, and Class members to an unreasonable risk of harm because they were foreseeable and probable victims of any inadequate security practices.

43. Equifax owed a duty of care not to subject Plaintiffs, along with their PII, and Class members to an unreasonable risk of harm because they were foreseeable and probable victims of any inadequate security practices.

44. Equifax owed numerous duties to Plaintiffs and to members of the Nationwide Class, including the following:

- a. to exercise reasonable care in obtaining, retaining, securing, safeguarding, deleting and protecting PII in its possession;

- b. to protect PII using reasonable and adequate security procedures and systems that are compliant with industry-standard practices; and
- c. to implement processes to quickly detect a data breach and to timely act on warnings about data breaches.

45. Equifax also breached its duty to Plaintiffs and the Class Members to adequately protect and safeguard PII by knowingly disregarding standard information security principles, despite obvious risks, and by allowing unmonitored and unrestricted access to unsecured PII. Furthering their dilatory practices, Equifax failed to provide adequate supervision and oversight of the PII with which they were and are entrusted, in spite of the known risk and foreseeable likelihood of breach and misuse, which permitted an unknown third party to gather PII of Plaintiffs and Class Members, misuse the PII and intentionally disclose it to others without consent.

46. Equifax knew, or should have known, of the risks inherent in collecting and storing personal identification information, the vulnerabilities of its data security systems, and the importance of adequate security.

47. Equifax knew, or should have known, that their data systems and networks did not adequately safeguard Plaintiffs' and Class Members' credit and personal identification information.

48. Equifax breached its duties to Plaintiffs and Class Members by failing to provide fair, reasonable, or adequate computer systems and data security practices to safeguard credit and personal identification information of Plaintiffs and Class Members.

49. Knowing the damage, a breach of its servers would cause millions of individuals, including Plaintiffs and Class members, Equifax had a duty to adequately protect their data systems and the PII contained thereon.

50. Equifax had a special relationship with Plaintiffs and Class members.

Plaintiffs' and Class members' willingness to entrust Equifax with their PII was predicated on the understanding that Equifax would take adequate security precautions. Moreover, only Equifax had the ability to protect its computer systems and servers, including the credit and personal identification information stored on them from attack.

51. Equifax's own conduct also created a foreseeable risk of harm to Plaintiffs and Class members and their PII. Equifax's misconduct included failing to: (1) secure its systems, despite knowing their vulnerabilities, (2) comply with industry standard security practices, (3) implement adequate system and event monitoring, and (4) implement the systems, policies, and procedures necessary to prevent this type of data breach.

52. Equifax also had independent duties under state and federal laws that required Equifax to reasonably safeguard Plaintiff's and Class members' Personal Information and promptly notify them about the data breach.

53. Equifax breached its duties to Plaintiffs and Class members in numerous ways, including:

- a. by failing to provide fair, reasonable, or adequate computer systems and data security practices to safeguard credit and personal identification information of Plaintiffs and Class members;
- b. by creating a foreseeable risk of harm through the misconduct previously described;
- c. by failing to implement adequate security systems, protocols and practices sufficient to protect Plaintiffs' and Class members' personal identification information both before and after learning of the Data Breach;

- d. by failing to comply with the minimum industry data security standards during the period of the Data Breach; and
- e. by failing to timely and accurately disclose that Plaintiffs' and Class members' credit and personal information had been improperly acquired or accessed.

54. Through Equifax's acts and omissions described in this Complaint, including Equifax's failure to provide adequate security and its failure to protect PII of Plaintiffs and Class members from being foreseeably captured, accessed, disseminated, stolen and misused, Equifax unlawfully breached its duty to use reasonable care to adequately protect and secure PII of Plaintiffs and Class members during the time it was within Equifax possession or control.

55. The law further imposes an affirmative duty on Equifax to timely disclose the unauthorized access and theft of the PII to Plaintiffs and the Class so that Plaintiffs and Class members can take appropriate measures to mitigate damages, protect against adverse consequences, and thwart future misuse of their credit and personal identification information.

56. Equifax breached its duty to notify Plaintiffs and Class Members of the unauthorized access by waiting many months after learning of the breach to notify Plaintiffs and Class Members and then by failing to provide Plaintiffs and Class Members information regarding the breach until September 2017. Instead, its executives disposed of at approximately \$2 million worth of shares in the company after Equifax learned of the data breach but before it was publicly announced. To date, Equifax has not provided sufficient information to Plaintiffs and Class Members regarding the extent of the unauthorized access and continues to breach its disclosure obligations to Plaintiffs and the Class.

57. Through Equifax's acts and omissions described in this Complaint, including Equifax's failure to provide adequate security and its failure to protect PII of Plaintiffs and Class Members from being foreseeably captured, accessed, disseminated, stolen and misused, Equifax unlawfully breached its duty to use reasonable care to adequately protect and secure PII of Plaintiffs and Class members during the time it was within Equifax's possession or control.

58. Further, through its failure to provide timely and clear notification of the Data Breach to consumers, Equifax prevented Plaintiffs and Class Members from taking meaningful, proactive steps to secure their financial data and bank accounts.

59. Upon information and belief, Equifax improperly and inadequately safeguarded PII of Plaintiffs and Class Members in deviation of standard industry rules, regulations, and practices at the time of the unauthorized access. Equifax's failure to take proper security measures to protect sensitive PII of Plaintiffs and Class members as described in this Complaint, created conditions conducive to a foreseeable, intentional criminal act, namely the unauthorized access of credit and personal identification information of Plaintiffs and Class members.

60. Equifax's conduct was grossly negligent and departed from all reasonable standards of care, including, but not limited to: failing to adequately protect the PII; failing to conduct regular security audits; failing to provide adequate and appropriate supervision of persons having access to credit and personal identification information of Plaintiffs and Class members; and failing to provide Plaintiffs and Class members with timely and sufficient notice that their sensitive PII had been compromised.

61. Neither Plaintiffs nor the other Class members contributed to the Data Breach and subsequent misuse of their credit and personal identification information as described in this Complaint.

62. As a direct and proximate cause of Equifax's conduct, Plaintiffs and the Class suffered damages including, but not limited to: damages arising from the unauthorized charges on their debit or credit cards or on cards that were fraudulently obtained through the use of the credit and personal identification information of Plaintiffs and Class Members; damages arising from Plaintiffs' inability to use their debit or credit cards because those cards were cancelled, suspended, or otherwise rendered unusable as a result of the Data Breach and/or false or fraudulent charges stemming from the Data Breach, including but not limited to late fees charges and foregone cash back rewards; damages from lost time and effort to mitigate the actual and potential impact of the Data Breach on their lives including, inter alia, by placing "freezes" and "alerts" with credit reporting agencies, contacting their financial institutions, closing or modifying financial accounts, closely reviewing and monitoring their credit reports and accounts for unauthorized activity, and filing police reports and damages from identity theft, which may take months if not years to discover and detect, given the far-reaching, adverse and detrimental consequences of identity theft and loss of privacy. The nature of other forms of economic damage and injury may take years to detect, and the potential scope can only be assessed after a thorough investigation of the facts and events surrounding the theft mentioned above.

**COUNT II NEGLIGENCE PER SE**

**(ON BEHALF OF PLAINTIFFS AND THE NATIONWIDE CLASS, OR,  
ALTERNATIVELY, PLAINTIFFS AND THE SEPARATE STATEWIDE  
CLASSES)**

63. Plaintiffs restate and reallege Paragraphs 1 through 59 as if fully set forth herein.

64. Section 5 of the FTC Act prohibits “unfair . . . practices in or affecting commerce,” including, as interpreted and enforced by the FTC, the unfair act or practice by businesses, such as Equifax, of failing to use reasonable measures to protect PII. The FTC publications and orders described above also form part of the basis of Equifax’s duty in this regard.

65. Equifax violated Section 5 of the FTC Act by failing to use reasonable measures to protect PII and not complying with applicable industry standards, as described in detail herein. Equifax’s conduct was particularly unreasonable given the nature and amount of PII it obtained and stored, and the foreseeable consequences of a data breach at a corporation such as Equifax, including, specifically, the immense damages that would result to Plaintiffs and Class Members.

66. Equifax’s violation of Section 5 of the FTC Act constitutes negligence per se.

67. Plaintiffs and Class Members are within the class of persons that the FTC Act was intended to protect.

68. The harm that occurred as a result of the Equifax Data Breach is the type of harm the FTC Act was intended to guard against. The FTC has pursued enforcement actions against businesses, which, as a result of their failure to employ reasonable data security measures and avoid unfair and deceptive practices, caused the same harm as that suffered by Plaintiffs and the Class.

69. As a direct and proximate result of Equifax's negligence per se, Plaintiffs and the Class have suffered, and continue to suffer, injuries damages arising from Plaintiffs' inability to use their debit or credit cards because those cards were cancelled, suspended, or otherwise rendered unusable as a result of the Data Breach and/or false or fraudulent charges stemming from the Data Breach, including but not limited to late fees charges and foregone cash back rewards; damages from lost time and effort to mitigate the actual and potential impact of the Data Breach on their lives including, inter alia, by placing "freezes" and "alerts" with credit reporting agencies, contacting their financial institutions, closing or modifying financial accounts, closely reviewing and monitoring their credit reports and accounts for unauthorized activity, and filing police reports and damages from identity theft, which may take months if not years to discover and detect, given the far-reaching, adverse and detrimental consequences of identity theft and loss of privacy.

**COUNT III NEGLIGENCE VIOLATION OF  
THE FAIR CREDIT REPORTING ACT  
(ON BEHALF OF PLAINTIFFS AND THE NATIONWIDE CLASS, OR,  
ALTERNATIVELY, PLAINTIFFS AND THE SEPARATE STATEWIDE  
CLASSES)**

70. Plaintiffs restate and reallege Paragraphs 1 through 66 as if fully set forth herein.

71. Equifax was negligent in failing to maintain reasonable procedures designed to limit the furnishing of consumer reports to the purposes outlined under section 1681b of the FCRA. Equifax's negligent failure to maintain reasonable procedures is supported by, among other things, former employees' admissions that Equifax's data security practices have deteriorated in recent years, and Equifax's numerous other data breaches in the past. Further, as an enterprise claiming to be an industry leader in data breach prevention,

Equifax was well aware of the importance of the measures organizations should take to prevent data breaches, yet failed to take them.

72. Equifax's negligent conduct provided a means for unauthorized intruders to obtain Plaintiffs' and the Nationwide Class members' PII and consumer reports for no permissible purposes under the FCRA.

73. Plaintiffs and the Nationwide Class member have been damaged by Equifax's negligent failure to comply with the FCRA. Therefore, Plaintiffs and each of the Nationwide Class member are entitled to recover "any actual damages sustained by the consumer." 15 U.S.C. § 1681o(a)(1).

74. Plaintiffs and the Nationwide Class member are also entitled to recover their costs of the action, as well as reasonable attorneys' fees. 15 U.S.C. § 1681o(a)(2).

**COUNT IV DECLARATORY JUDGMENT  
(ON BEHALF OF PLAINTIFFS AND THE NATIONWIDE CLASS, OR,  
ALTERNATIVELY, PLAINTIFFS AND THE SEPARATE STATEWIDE  
CLASSES)**

75. Plaintiffs restate and reallege Paragraphs 1 through 71 as if fully set forth herein.

76. As previously alleged, Plaintiffs and Class members entered into an implied contract that required Equifax to provide adequate security for the PII it collected from their payment card transactions. As previously alleged, Equifax owes duties of care to Plaintiffs and Class members that require it to adequately secure PII.

77. Equifax still possesses PII pertaining to Plaintiffs and Class members.

78. Equifax has made no announcement or notification that it has remedied the vulnerabilities in its computer data systems, and, most importantly, its systems.

79. Accordingly, Equifax has not satisfied its contractual obligations and legal duties to Plaintiffs and Class members. In fact, now that Equifax's lax approach towards data security has become public, the PII in its possession is more vulnerable than previously.

80. Actual harm has arisen in the wake of the Equifax Data Breach regarding Equifax's contractual obligations and duties of care to provide data security measures to Plaintiffs and Class members.

81. Plaintiffs, therefore, seek a declaration that (a) Equifax's existing data security measures do not comply with its contractual obligations and duties of care, and (b) in order to comply with its contractual obligations and duties of care, Equifax must implement and maintain reasonable security measures, including, but not limited to:

a. engaging third-party security auditors/penetration testers as well as internal security personnel to conduct testing, including simulated attacks, penetration tests, and audits on Equifax's systems on a periodic basis, and ordering Equifax to promptly correct any problems or issues detected by such third-party security auditors;

b. engaging third-party security auditors and internal personnel to run automated security monitoring;

c. auditing, testing, and training its security personnel regarding any new or modified procedures;

d. segmenting PII by, among other things, creating firewalls and access controls so that if one area of Equifax is compromised, hackers cannot gain access to other portions of Equifax systems;

e. purging, deleting, and destroying in a reasonable secure manner PII not

necessary for its provisions of services;

- f. conducting regular database scanning and securing checks;
- g. routinely and continually conducting internal training and education to inform internal security personnel how to identify and contain a breach when it occurs and what to do in response to a breach; and
- h. educating its customers about the threats they face as a result of the loss of their financial and personal information to third parties, as well as the steps Equifax customers must take to protect themselves.

**PRAYER FOR RELIEF**

**WHEREFORE**, Plaintiffs, individually and on behalf of all Class members proposed in this Complaint, respectfully request that the Court enter judgment in their favor and against EQUIFAX as follows:

- a. For an Order certifying the Classes, as defined herein, and appointing Plaintiffs and their Counsel to represent the Nationwide Class, or in the alternative the separate Statewide Classes;
- b. An order to preserve all documents and information (and electronically stored information) pertaining to this case,
- c. For equitable relief enjoining Equifax from engaging in the wrongful conduct complained of herein pertaining to the misuse and/or disclosure of Plaintiffs' and Class members' credit and personal identification information, and from refusing to issue prompt, complete and accurate disclosures to the Plaintiffs and Class members;
- d. For equitable relief compelling Equifax to use appropriate cyber security methods and policies with respect to consumer data collection, storage and

protection and to disclose with specificity to Class members the type of credit and personal identification information compromised;

- e. For an award of damages, as allowed by law in an amount to be determined;
- f. For an award of attorneys' fees costs and litigation expenses, as allowable by law;
- g. For prejudgment interest on all amounts awarded; and
- h. Such other and further relief as this court may deem just and proper.

THIS, 12<sup>th</sup> day of September 2017.

**RESPECTFULLY FILED,**

**DORSEY & GATES, PLLC**

/s Tanisha M. Gates  
**Tanisha M. Gates, MSB No. 102071**  
**Vallrie L. Dorsey, MSB No. 102538**  
P.O. Box 158  
Belzoni, MS 39038  
P: (662) 247-2449  
F: (662) 247-2437

[tgates@dorseygates.com](mailto:tgates@dorseygates.com)  
[vdorsey@dorseygates.com](mailto:vdorsey@dorseygates.com)

**DANIEL E. MORRIS LAW FIRM, PLLC**

/s Daniel E. Morris, Esq.  
**Daniel E. Morris, MSB No. 102723**  
P.O. Box 40811  
Baton Rouge, LA 70835  
P: (888) 966-7747 (888-9-MORRIS)  
F: (877) 966-7747 (877-9-MORRIS)

[danielmorris@demlawfirm.com](mailto:danielmorris@demlawfirm.com)